CLAIMS

What is claimed is:

1. A method comprising:

reading an encrypted data block from memory;

regenerating, during reading of the encrypted data block, a keystream used to encrypt the data block according to one or more stored criteria of the data block; and

once reading of the encrypted data block is complete, decrypting the encrypted data block according to the generated keystream.

2. The method of claim 1, wherein reading the encrypted data block comprises:

receiving a request for the encrypted data block; and

reading the encrypted data block from a random access memory.

3. The method of claim 1, wherein re-generating the keystream comprises:

identifying an initial portion of an initialization vector used to encrypt the data block according to a page containing the encrypted data block;

identifying a remaining portion of the initialization vector used to encrypt the data block according to a block number of the data block; and

recomputing the keystream according to the identified initial portion of initialization vector and the identified remaining portion of the initialization vector and a secret key.

4. The method of claim 3, wherein computing the keystream comprises:

selecting a stored page initialization vector value according to a page containing the encrypted data block and a block number of the encrypted data block from an on-chip data structure containing one or more unique page initialization vectors;

selecting a stored C-bit counter value according to the block number of the encrypted data block;

reforming the initialization vector used to encrypt the data block according to the page initialization vector value, the C-bit counter value and (N - C) most significant bits of an address of the encrypted data block, where the address is an N-bit address; and

encrypting the formed initialization vector using the secret key to form the keystream.

5. The method of claim 1, wherein decrypting the encrypted data block is performed within a single clock cycle.

6. An article of manufacture including a machine readable medium having stored thereon instructions which may be used to program a system to perform a method, comprising:

reading an encrypted data block from memory;

regenerating, during reading of the encrypted data block, a keystream used to encrypt the data block according to one or more stored criteria of the data block; and

once reading of the encrypted data block is complete, decrypting the encrypted data block according to the generated keystream.

7. The article of manufacture of claim 6, wherein prior to receiving the request the method comprises:

receiving a request for the encrypted data block; and

reading the encrypted data block from a random access memory.

8. The article of manufacture of claim 6, wherein prior to receiving the request the method comprises:

identifying an initial portion of an initialization vector used to encrypt the data block according to a page containing the encrypted data block;

identifying a remaining portion of the initialization vector used to encrypt the data block according to a block number of the data block; and

recomputing the keystream according to the identified initial portion of initialization vector and the identified remaining portion of the initialization vector and a secret key.

9. The article of manufacture of claim 8, wherein prior to receiving the request the method comprises:

selecting a stored page initialization vector value according to a page containing the encrypted data block and a block number of the encrypted data block from an on-chip data structure containing one or more unique page initialization vectors;

selecting a stored C-bit counter value according to the block number of the encrypted data block;

reforming the initialization vector used to encrypt the data block according to the page initialization vector value, the C-bit counter value and (N - C) most significant bits of an address of the encrypted data block, where the address is an N-bit address; and

encrypting the formed initialization vector using the secret key to form the keystream.

10. The article of manufacture of claim 6, wherein decrypting the selected data block is performed within a single clock cycle.

11. A method comprising:

computing an initialization vector for a data block according to one or more criteria of the data block,

storing the criteria of the data block used to compute the initialization vector for the data block;

computing a keystream from the initialization vector and a secret key;

encrypting the data block according to the keystream; and

storing the encrypted data block within memory.

12. The method of claim 11, wherein computing the initialization vector comprises:

receiving a write request for the data block;

identifying a page containing the data block;

forming a page initialization vector according to the page containing the data block as the initialization vector of the data block.

13. The method of claim 11, wherein computing the initialization vector comprises:

receiving a write request for the data block;

identifying a page containing the data block and a block number of the data block within the page;

forming a page initialization vector according to the page containing the data block and the block number of the encrypted data block;

forming a block initialization vector according to the block number of the data block; and

combining the page initialization vector and the block initialization vector to form the initialization vector.

14. The method of claim 13, wherein forming the page initialization vector comprises:

identifying a plurality of page initialization vectors assigned to the page containing the data block from an on-chip data structure containing one or more unique page initialization vectors; and

selecting a page initialization vector according to a page counter value for the page containing the data block.

15. The method of claim 13, wherein forming the block initialization vector comprises:

selecting a block counter value for page writes to the page containing the data block as the block initialization vector.

16. The method of claim 11, wherein combining to form the initialization vector comprises:

selecting a stored page initialization vector value according to a page containing the unencrypted data block from an on-chip data structure containing one or more unique page initialization vectors;

selecting a stored C-bit counter value according to the block number of the encrypted data block;

forming the initialization vector used to encrypt the data block according to the page initialization vector value, the C-bit counter value and (N - C) most significant bits of an address of the encrypted data block, where the address is an N-bit address; and

encrypting the formed initialization vector using the secret key to form the keystream.

17. The method of claim 11, wherein computing the keystream comprises:

providing the initialization vector and the secret key to one of a stream cipher and a block cipher to generate the keystream.

18. The method of claim 11, further comprising:

identifying a data block having a least recent initialization vector;

computing a unique initialization vector for the identified initialization vector; and

re-encrypting the identified data block according to a keystream generated from the unique initialization vector and a secret key.

19. The method of claim 18, wherein computing the unique initialization vector comprises:

identifying a current page initialization vector value according to a page counter value of a page containing the identified data block; and

replacing a page initialization vector portion of the identified initialization vector with the current page initialization vector value to form the unique initialization vector.

20. The method of claim 11, wherein storing the initialization vector comprises:

identifying a page counter value used to select a page vector value of the initialization vector;

identifying a block counter value used to form a block vector value of the initialization vector; and

storing the page counter value and the block counter value within an encryption page structure according to a block number of the data block.

21. A processor comprising:

memory encryption logic to store one or more criteria of a data block used to compute an initialization vector for the data block, encrypt the data block according to a keystream computed from the initialization vector and a secret key, and store the encrypted data block within memory; and

memory decryption logic to regenerate, during an encrypted data block read, a keystream used to encrypt the data block according to one or more stored criteria of the data block and decrypt the encrypted data block using the regenerated keystream.

22. The apparatus of claim 21, wherein the encryption logic further comprises:

a memory including an encryption page structure having a page data structure containing one or more unique page initialization vector values used in formation of

initialization vectors, and a block data structure used to store an index value to the page data structure and block data structure used to form an initialization vector for recomputation of a keystream and to encrypt data blocks.

23. The apparatus of claim 21, wherein the encryption logic further comprises

recode logic to identify a data block having a least recent initialization vector, recompute a unique initialization vector for the identified initialization vector, and re-encrypt the identified data block according to a keystream generated from the unique initialization vector and a secret key.

24. The apparatus of claim 21, wherein the decrypt logic decrypts encrypted data blocks within a single clock cycle using an exclusive-OR operation.

25. the apparatus of claim 21, wherein the memory is one of random access memory and disk memory.

26. A system comprising:

a random access memory (RAM);

a chipset coupled to the memory; and

a processor coupled to the chipset, the processor including:

memory encryption logic to store one or more criteria of a data block used to compute an initialization vector for the data block, encrypt the data block according to the keystream computed the initialization vector and a secret key, and store the encrypted data block within the memory, and

memory decryption logic to regenerate, during an encrypted data block read from the memory, a keystream used to encrypt the data block according to one or more stored criteria of the data block and decrypt the encrypted data block using the regenerated keystream.

27. The system of claim 26, wherein the encryption logic further comprises:

a memory including an encryption page structure having a page data structure containing one or more unique page initialization vector values used in formation of initialization vectors, and a block data structure used to store an index value to the page data structure and block data structure used to form an initialization vector for recomputation of a keystream and to encrypt data blocks.

28. The system of claim 26, wherein the encryption logic further comprises recode logic to identify a data block having a least recent initialization vector, replace the identified initialization vector with a current initialization vector, and re-encrypt the identified data block according to a keystream generated from the current initialization vector and a secret key.

29. The system of claim 26, wherein the decrypt logic decrypts encrypted data blocks within a single clock cycle using an exclusive-OR operation.

30. The system of claim 26, wherein the RAM memory is double data rate (DDR) synchronous data RAM (SDRAM)

31. An article of manufacture including a machine readable medium having stored thereon instructions which may be used to program a system to perform a method, comprising:

computing an initialization vector for a data block according to one or more criteria of the data block,

storing the criteria of the data block used to compute the initialization vector for the data block;

computing a keystream from the initialization vector and a secret key;

encrypting the data block according to the keystream; and

storing the encrypted data block within memory.

32. The article of manufacture of claim 31, wherein computing the initialization vector comprises:

receiving a write request for the data block;

identifying a page containing the data block and a block number of the data block within the page;

forming a page initialization vector according to the page containing the data block and the block number of the encrypted data block;

forming a block initialization vector according to the block number of the data block; and

combining the page initialization vector and the block initialization vector to form the initialization vector.

33. The article of manufacture of claim 31, wherein combining to form the initialization vector comprises:

selecting a stored page initialization vector value according to a page containing the unencrypted data block and the block number of the encrypted data block from an on-chip data structure containing one or more unique page initialization vectors;

selecting a stored C-bit counter value according to a block number of the encrypted data block;

forming the initialization vector used to encrypt the data block according to the page initialization vector value, the C-bit counter value and (N - C) most significant bits of an address of the encrypted data block, where the address is an N-bit address; and

encrypting the formed initialization vector using the secret key to form the keystream.

34. The article of manufacture of claim 31, wherein the method further comprises:

identifying a data block having a least recent initialization vector;

computing a unique initialization vector from the identified initialization vector; and

re-encrypting the identified data block according to a keystream generated from the unique initialization vector and a secret key.

35. The article of manufacture of claim 34, computing the unique initialization vector comprises:

identifying a current page initialization vector value according to a page counter value of a page containing the identified data block; and

replacing a page initialization vector portion of the identified initialization vector with the current page initialization vector value to form the unique initialization vector.